Bigger US role against companies' cyberthreats?

February 6 2012, By LOLITA C. BALDOR , Associated Press

In this Sept. 21, 2011, file photo Senate Homeland Security and Governmental Affairs Chairman Sen. Joseph Lieberman, I-Conn. presides over the committee's hearing on Capitol Hill in Washington. A developing Senate plan that would bolster the government's ability to regulate the computer security of companies that run critical industries is drawing strong opposition from businesses that say it goes too far and security experts who believe it should have even more teeth. "But where the market has failed, and critical systems are insecure, the government has a responsibility to step in," said Leiberman. (AP Photo Manuel Balce Ceneta, File)

(AP) -- A developing Senate plan that would bolster the government's ability to regulate the computer security of companies that run critical industries is drawing strong opposition from businesses that say it goes too far and security experts who believe it should have even more teeth.

Legislation set to come out in the days ahead is intended to ensure that

computer systems running power plants and other essential parts of the country's infrastructure are protected from hackers, terrorists or other criminals. The Department of Homeland Security, with input from businesses, would select which companies to regulate; the agency would have the power to require better computer security, according to officials who described the bill. They spoke on condition of anonymity because lawmakers have not finalized all the details.

Those are the most contentious parts of legislation designed to boost cybersecurity against the constant attacks that target U.S. government, corporate and personal computer networks and accounts. Authorities are increasingly worried that cybercriminals are trying to take over systems that control the inner workings of water, electrical, nuclear or other power plants.

That was the case with the Stuxnet computer worm, which targeted Iran's nuclear program in 2010, infecting laptops at the Bushehr nuclear power plant.

As much as 85 percent of America's critical infrastructure is owned and operated by private companies

The emerging proposal isn't sitting well with those who believe it gives Homeland Security too much power and those who think it's too watered down to achieve real security improvements.

One issue under debate is how the bill narrowly limits the industries that would be subject to regulation.

Summaries of the bill refer to companies with systems "whose disruption could result in the interruption of life-sustaining services, catastrophic economic damage or severe degradation of national security capabilities."

Critics suggest that such limits may make it too difficult for the government to regulate those who need it.

There are sharp disagreements over whether Homeland Security is the right department to enforce the rules and whether it can handle the new responsibilities. U.S. officials familiar with the debate said the department would move gradually, taking on higher priority industries first.

"The debate taking place in Congress is not whether the government should protect the American people from catastrophic harms caused by cyberattacks on critical infrastructure, but which entity can do that most effectively," said Jacob Olcott, a senior cybersecurity expert at Good Harbor Consulting.

Under the legislation, Homeland Security would not regulate industries that are under the authority of an agency, such as the Nuclear Regulatory Commission, with jurisdiction already over cyber issues.

"Where the market has worked, and systems are appropriately secure, we don't interfere," said Sen. Joe Lieberman, I-Conn., chairman of the Senate Homeland Security and Governmental Affairs Committee. "But where the market has failed, and critical systems are insecure, the government has a responsibility to step in."

The bill, written largely by the Senate Commerce, Science and Transportation Committee and the Senate homeland panel, is also notable for what it does not include: a provision that would give the president authority to shut down Internet traffic to compromised Web sites during a national emergency. This `"kill switch" idea was discussed in early drafts, but drew outrage from corporate leaders, privacy advocates and Internet purists who believe cyberspace should remain an untouched digital universe.

While the Senate is pulling together one major piece of cybersecurity legislation, the House has several bills that deal with various aspects of the issue.

A bill from a House Homeland Security subcommittee doesn't go as far as the Senate's in setting the government's role. Still, it would require DHS to develop cybersecurity standards and work with industry to meet them.

"We know voluntary guidelines simply have not worked," said Rep. Jim Langevin, D-R.I. "For the industries upon which we most rely, government has a role to work with the private sector on setting security guidelines and ensuring they are followed."

Stewart Baker, a former assistant secretary at Homeland Security, said the government must get involved to force companies to take cybersecurity more seriously.

Concerns about federal involvement, he said, belie the fact that computer breaches over the past several years make it clear that hackers and other governments, such as China and Russia, are already inside many industry networks.

"They already have governments in their business, just not the U.S.," said Baker. "For them to say they don't want this suggests they don't really understand how bad this problem is."

Industry groups have lobbied against the Senate bill's regulatory powers and say new mandates will drive up costs without increasing security.

They say businesses are trying to secure their networks and need legal protections built into the law so they can share information with authorities without risking antitrust or privacy violations.

In a letter to lawmakers this past week, the U.S. Chamber of Commerce said any additional regulations would be counterproductive and force businesses to shift their focus from security to compliance.

Liesyl Franz, a vice president at TechAmerica, which represents about 1,200 companies, said businesses would prefer to work with the government to enhance security rather than face more regulations. She said companies coping with the potential security risks, market consequences, and damage to corporate reputations, are defending against cyberthreats.

Senior national security officials were on Capitol Hill last week to talk to senators about the growing cybersecurity threat. After the meeting, Sen. Susan Collins, R-Maine, said she's always had a sense of urgency about it, adding, "I hope the briefing gives that same sense of urgency to members to put aside turf battles."

She said senators are reviewing concerns raised by the Chamber about the bill.